

AO 106A (08/18) Application for a Warrant by Telephone or Other Reliable Electronic Means

**FILED**

## UNITED STATES DISTRICT COURT

UNITED STATES DISTRICT COURT  
LAS CRUCES, NEW MEXICOfor the  
District of New Mexico

OCT 25 2023

MITCHELL R. ELLERS  
CLERK OF COURT

Case No. 23 - 2026 MR

## In the Matter of the Search of

(Briefly describe the property to be searched  
or identify the person by name and address)IN THE MATTER OF THE SEARCH OF INFORMATION ASSOCIATED WITH  
IMEI 352130214308917, IMEI 352130214215138, TELEPHONE NUMBER (575)  
635-9530, martinez.michael1107@yahoo.com and  
mmartinez@villageofhatch.org (the "ACCOUNTS")  
THAT IS STORED AT PREMISES CONTROLLED BY APPLE INC.

## APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

See Attachment A.

located in the Northern District of California or elsewhere, there is now concealed (identify the person or describe the property to be seized):

See Attachment B.

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
- ☒ contraband, fruits of crime, or other items illegally possessed;
- ☒ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	Offense Description
18 U.S.C. §§ 242, 250	Deprivation of Rights Under Color of Law
18 U.S.C. §1512(b)(3)	Witness Tampering
18 U.S.C. §1512(c)(1)	Obstruction of Justice

The application is based on these facts:

See Attachment C.

☒ Continued on the attached sheet.☐ Delayed notice of \_\_\_\_\_ days (give exact ending date if more than 30 days: \_\_\_\_\_) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Applicant's signature

Armida Maria Macmanus, FBI Special Agent

Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by  
telephone (specify reliable electronic means).

Date: October 25, 2023

City and state: Las Cruces, New Mexico

Judge's signature

Jerry H. Ritter, U.S. Magistrate Judge

Printed name and title

**ATTACHMENT A**

**Property to Be Searched**

This warrant applies to information associated with IMEI 352130214308917, IMEI 352130214215138, telephone number (575) 635-9530, [martinez.michael1107@yahoo.com](mailto:martinez.michael1107@yahoo.com) and [mmartinez@villageofhatch.org](mailto:mmartinez@villageofhatch.org) (the "ACCOUNTS") that is stored at premises owned, maintained, controlled, or operated by Apple Inc., a company headquartered at One Apple Park Way, Cupertino, California.

**ATTACHMENT B**

**Particular Things to be Seized**

**I. Information to be disclosed by Apple Inc. (“Apple”)**

To the extent that the information described in Attachment A is within the possession, custody, or control of Apple, regardless of whether such information is located within or outside of the United States, and including any emails, records, files, logs, or information that has been deleted but is still available to Apple, or has been preserved pursuant to the request made under 18 U.S.C. § 2703(f) on September 22, 2023, Apple is required to disclose the following information to the government for each account or identifier listed in Attachment A, for the time period of **April 29, 2023 to September 21, 2023**, unless otherwise indicated:

- a. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers, email addresses (including primary, alternate, rescue, and notification email addresses, and verification information for each email address), the date on which the account was created, the length of service, the IP address used to register the account, account status, associated devices, methods of connecting, and means and source of payment (including any credit or bank account numbers);
- b. All records or other information regarding the devices associated with, or used in connection with, the account (including all current and past trusted or authorized iOS devices and computers, and any devices used to access Apple services), including serial numbers, Unique Device Identifiers (“UDID”), Advertising Identifiers (“IDFA”), Global Unique Identifiers (“GUID”), Media Access Control (“MAC”) addresses, Integrated Circuit Card ID numbers (“ICCID”), Electronic Serial Numbers (“ESN”), Mobile Electronic Identity Numbers (“MEIN”), Mobile Equipment Identifiers (“MEID”), Mobile Identification Numbers (“MIN”), Subscriber

Identity Modules (“SIM”), Mobile Subscriber Integrated Services Digital Network Numbers (“MSISDN”), International Mobile Subscriber Identities (“IMSI”), and International Mobile Station Equipment Identities (“IMEI”);

c. The contents of all emails associated with the account, including stored or preserved copies of emails sent to and from the account (including all draft emails and deleted emails), the source and destination addresses associated with each email, the date and time at which each email was sent, the size and length of each email, and the true and accurate header information including the actual IP addresses of the sender and the recipient of the emails, and all attachments;

d. The contents of all instant messages associated with the account, including stored or preserved copies of instant messages (including iMessages, SMS messages, and MMS messages) sent to and from the account (including all draft and deleted messages), the source and destination account or phone number associated with each instant message, the date and time at which each instant message was sent, the size and length of each instant message, the actual IP addresses of the sender and the recipient of each instant message, and the media, if any, attached to each instant message;

e. The contents of all files and other records stored on iCloud, including all iOS device backups, all Apple and third-party app data, all files and other records related to iCloud Mail, iCloud Photo Sharing, My Photo Stream, iCloud Photo Library, iCloud Drive, iWork (including Pages, Numbers, Keynote, and Notes), iCloud Tabs and bookmarks, and iCloud Keychain, and all address books, contact and buddy lists, notes, reminders, calendar entries, images, videos, voicemails, device settings, and bookmarks;

f. All activity, connection, and transactional logs for the account (with associated IP addresses including source port numbers), including FaceTime call invitation logs, messaging and capability query logs (including iMessage, SMS, and MMS messages), mail logs, iCloud logs, iTunes Store and App Store logs (including purchases, downloads, and updates of Apple and third-party apps), My Apple ID and iForgot logs, sign-on logs for all Apple services, Game Center logs, Find My and AirTag logs, logs associated with web-based access of Apple services (including all associated identifiers), and logs associated with iOS device purchase, activation, and upgrades;

g. All records and information regarding locations where the account or devices associated with the account were accessed, including all data stored in connection with AirTags, Location Services, Find My, and Apple Maps;

h. All records pertaining to the types of service used;

i. All records pertaining to communications between Apple and any person regarding the account, including contacts with support services and records of actions taken; and

j. All files, keys, or other information necessary to decrypt any data produced in an encrypted form, when available to Apple (including, but not limited to, the keybag.txt and fileinfolist.txt files).

Apple is hereby ordered to disclose the above information to the government within **fourteen** days of issuance of this warrant.

## **II. Information to be seized by the government**

All information described above in Section I that constitutes fruits, evidence, and instrumentalities of violations of 18 U.S.C. §§ 242, 250, Deprivation of Rights Under Color of Law, and 18 U.S.C. § 1512(b)(3), Witness Tampering, and 18 U.S.C. § 1512(c)(1), Obstruction of Justice, those violations involving Michael Andrew Martinez and occurring on and after April 30, 2023, including, for each account or identifier listed on Attachment A, information pertaining to the following matters:

- a. All records, images, communications, or information, however maintained, relating to sexual harassment, sexual assault, rape, and bondage of women;
- b. All records, images, communications, or information, however maintained, reflecting the planning and execution of (1) a sexual assault or other sexual misconduct, (2) the destruction of evidence relating to sexual assault or other sexual misconduct; and (3) attempts to influence witnesses to not report or believe accounts of sexual assault or other sexual misconduct;
- c. All records, images, communications, or information, however maintained, reflecting the planning or execution of the destruction of (1) a body worn camera and the footage contained therein and of (2) a dashboard vehicle camera and the footage contained therein;
- d. All records, images, communications, or information, however maintained, relating to acts of sexual assault or other sexual misconduct committed by Michael Andrew Martinez;
- e. Any and all records of communications between Michael Andrew Martinez and any individual arrested and detained by Martinez in his capacity as a law enforcement officer;

- f. Photographs or videos of sexual assaults or acts of violence perpetrated against persons in custody and/or women who are restrained;
- a. Evidence of activity from April 29, 2023 to September 21, 2023 that evidences, indicates, or otherwise establishes that Michael Andrew Martinez sexually assaulted Victim and tampered with and obstructed justice in furtherance of the crimes he committed.
- b. Evidence indicating how and when the Apple iPhone account was accessed or used, to determine the geographic and chronological context of account access, use, and events relating to the crime under investigation and to the account subscriber;
- c. Evidence indicating the Apple iPhone account owner's state of mind as it relates to the crimes under investigation;
- d. The identity of the person(s) who created or used the user ID, including records that help reveal the whereabouts of such person(s).
- e. The identity of the persons who communicated with the user ID about matters relating to the sexual assault of Victim or other women, the tampering and destruction of evidence, and obstruction of justice, including records that help reveal those persons whereabouts.

This warrant authorizes a review of electronically stored information, communications, other records, and information disclosed pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the FBI shall deliver a complete copy of

the disclosed electronic data to the custody and control of attorneys for the government and their support staff for their independent review.



IN THE UNITED STATES DISTRICT COURT  
FOR THE DISTRICT OF NEW MEXICO

IN THE MATTER OF THE SEARCH OF  
INFORMATION ASSOCIATED WITH IMEI  
352130214308917, IMEI 352130214215138,  
TELEPHONE NUMBER (575) 635-9530,  
[martinez.michael1107@yahoo.com](mailto:martinez.michael1107@yahoo.com) and  
[mmartinez@villageofhatch.org](mailto:mmartinez@villageofhatch.org) (the  
"ACCOUNTS")  
THAT IS STORED AT PREMISES  
CONTROLLED BY APPLE INC.

Case No. 23-mj-1430-DLM

**AFFIDAVIT IN SUPPORT OF  
AN APPLICATION FOR A SEARCH WARRANT**

I, Armida Maria Macmanus, being first duly sworn, hereby depose and state as follows:

**INTRODUCTION AND AGENT BACKGROUND**

1. I make this affidavit in support of an application for a search warrant for information associated with certain accounts that are stored at premises owned, maintained, controlled, or operated by Apple Inc. ("Apple"), an electronic communications service and/or remote computing service provider headquartered at One Apple Park Way, Cupertino, California. The information to be searched is described in the following paragraphs and in Attachment A. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require Apple to disclose to the government copies of the information (including the content of communications) further described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

2. I am a Special Agent with the Federal Bureau of Investigation ("FBI") and have been since November 2005. I am currently assigned as a Special Agent for the Albuquerque

Division at the Las Cruces Resident Agency in Las Cruces, New Mexico. I am classified, trained, and employed as a federal law enforcement officer with statutory arrest authority charged with conducting criminal investigations of alleged violations of federal criminal statutes, including violations of Title 18 of the United States Code. My experience as a Special Agent includes but is not limited to: conducting physical surveillance; interviewing witnesses; writing affidavits for and executing search warrants; working with undercover agents and informants; issuing administrative and federal grand jury subpoenas; and analyzing financial records, telephone records, and data derived from the use of pen registers and trap and traces; and assisting in wiretap investigations. I have conducted or participated in investigations of subjects alleged to have violated 18 U.S.C. § 242, Deprivation of Rights Under Color of Law, and 18 U.S.C. § 1512, Witness Tampering and Obstruction of Justice.

3. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

4. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that evidence of violations of 18 U.S.C. §§ 242, 250, Deprivation of Rights Under Color of Law and 18 U.S.C. § 1512(b)(3), Witness Tampering, and 18 U.S.C. § 1512(c)(1), Obstruction of Justice have been committed by Michael Andrew Martinez. There is also probable cause to search the information described in Attachment A for evidence, instrumentalities, and/or fruits of these crimes further described in Attachment B.

#### **JURISDICTION**

5. This Court has jurisdiction to issue the requested warrant because it is “a court of competent jurisdiction” as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A), &

(c)(1)(A). Specifically, the Court is “a district court of the United States . . . that has jurisdiction over the offense being investigated.” 18 U.S.C. § 2711(3)(A)(i).

**PROBABLE CAUSE**

6. On or about September 15, 2023, the FBI received information that Michael Andrew Martinez (“Martinez”), while serving in his capacity as a deputy with the Doña Ana Sheriff’s Office (“DASO”), had sexually assaulted an adult female in custody (hereinafter “Victim”) on April 30, 2023, thereby depriving the Victim of her civil rights. The FBI also received information that in the hours or days following the sexual assault, Martinez attempted to destroy evidence of the sexual assault, thereby obstructing justice. It was determined that the criminal conduct occurred in Las Cruces, New Mexico, within the District of New Mexico. I am the case agent assigned to the ongoing federal investigation.

7. The initial investigation into Martinez’s sexual misconduct first arose from Martinez himself calling a DASO sergeant (hereinafter “Witness 1”) on May 2, 2023, claiming that he had just gone into his DASO patrol vehicle and noticed that the center console had been damaged and that his Global Positioning System (“GPS”) device was laying on his dashboard. Martinez further claimed that his patrol vehicle’s tactical radio and WatchGuard DVR system and WatchGuard monitor had been destroyed.<sup>1</sup> Based on my investigation, I know that the WatchGuard DVR system stores video footage from cameras inside the patrol car, including, as pertinent here, video footage from the dash-mounted camera and the rear seat camera. After

---

<sup>1</sup> I conducted an online search of the WatchGuard DVR system and learned that it is an integrated evidence-gathering and archiving system. This system, or it’s comparable alternative, is used by the DASO to capture law enforcement events with cameras and recorders such as the Motorola Solutions 4RE® in-car video system (WatchGuard DVR system) with V300 body-worn camera.

receiving this call, Witness 1 responded to Martinez's residence in Doña Ana County to investigate.

8. Upon arriving at Martinez's residence, Witness 1 spoke to Martinez who reiterated his claims about noticing the damage to the interior of his patrol vehicle and added that it also appeared that someone had opened and rummaged through his glove compartment. Witness 1 inspected the patrol vehicle and observed that the tactical radio, the WatchGuard DVR system, and the WatchGuard monitor were either damaged or destroyed. Martinez was ordered to return the vehicle to the DASO, so that the recovery of stored data within the WatchGuard DVR system could be attempted and reviewed for possible evidence of the alleged robbery.

9. The next day, May 3, 2023, Witness 1 contacted a lieutenant with the DASO Professional Standards Division (hereinafter "Witness 2"), who performs investigations of employees, due to the suspicious circumstances surrounding the DASO issued property that was damaged in and missing from Martinez's patrol vehicle. Witness 1 told Witness 2 that his investigation revealed no forced entry into Martinez's patrol vehicle and that the only item missing from the vehicle was Martinez's WatchGuard body worn DVR camera. On May 11, 2023, the DASO pulled the WatchGuard DVR from Martinez's patrol unit, and, on June 22, 2023, sent it to WatchGuard (Motorola). On August 21, 2023, WatchGuard sent the DASO a thumb drive containing videos recovered from Martinez's damaged WatchGuard DVR.

10. On August 30, 2023, Witness 2 reviewed the recovered videos, including one video which showed Martinez sexually assaulting Victim while she was in Martinez's custody, handcuffed and restrained with a seatbelt inside the prisoner compartment of Martinez's patrol unit. Witness 2 notified his chain of command, and on August 31, 2023, the DASO terminated

Martinez's employment. Approximately two weeks later, the FBI was notified, and my federal investigation ensued.

11. The investigation has thus far established that on April 30, 2023, while on duty as a DASO deputy, Martinez, wearing his full uniform and patrolling in a DASO marked patrol vehicle, responded to a car accident on Snow Road and Mesilla Dam Road in Doña Ana County, New Mexico. Martinez approached a car that had struck a tree. Two females stood near the car, one of which was the Victim, who was the registered owner of the vehicle. Further investigation revealed the Victim was the driver of the car during the accident.

12. After speaking with Victim, Martinez detained Victim for Driving Under the Influence of Intoxicating Liquor or Drugs (NM 66-8-102A) and Careless Driving (NM 66-8-114A). Martinez handcuffed Victim and placed her inside his patrol vehicle, a 2017 Chevrolet Tahoe, bearing New Mexico license plate G99453. Martinez read Victim the Implied Consent Advisory, and she agreed to produce a breath sample. Martinez then transported Victim to the DASO headquarters where he administered a breathalyzer test, which produced a first sample of 0.04 and a second sample that was insufficient. Victim remained inside a holding cell while Martinez completed requisite paperwork. Afterwards, Martinez placed Victim, who remained handcuffed, back inside his patrol vehicle.

13. Martinez next transported Victim to the Mountain View Medical Center in Las Cruces, New Mexico, to obtain a medical clearance. Once said medical clearance was obtained, Martinez put Victim, who was still handcuffed with her hands restrained behind her back, back into his patrol vehicle. Martinez then secured Victim's seatbelt, further restraining her, before sexually assaulting Victim. After sexually assaulting Victim, Martinez transported her to the Doña Ana County Detention Center and booked her into the facility.

14. As part of my investigation, I obtained and reviewed videos recovered from Martinez's patrol vehicle's WatchGuard DVR. The following is a summary of the video footage capturing Martinez's sexual assault of Victim. The video footage begins with a banner that reads, "Dep. Michael Martinez 04-30-2023 @0335 Hrs. Backseat.mp4." The video footage next captures Victim seated and seat-belted in the caged prisoner compartment of Martinez's patrol vehicle. Victim is wearing a light-colored hoodie and shorts and her hands are behind her back, apparently handcuffed. Martinez and Victim engage in casual conversation during the transport. After approximately 15 minutes of recorded video footage, Martinez stops his patrol vehicle (based on my investigation, I know Martinez stopped at the Mountain View Medical Center), opens the rear passenger side door, and releases Victim's seatbelt. Victim gets out of the vehicle and Martinez shuts the door. A little over two hours later, video footage captures Martinez's patrol vehicle's rear passenger side door reopen, and Victim gets back inside the caged prisoner compartment. Victim's hands are still behind her back, apparently handcuffed.

15. Video footage then captures Martinez ask Victim if she is ok and she appears to respond, "Yes, Sir," as Martinez places his right hand on Victim's upper right thigh. Martinez then places his left hand briefly on the inside of Victim's upper right thigh area. Seconds later, Martinez fastens Victim's seatbelt—further restraining her—and places his hand again on her upper right thigh between her legs for a moment. Martinez then moves Victim's thighs apart and places his hand on or near her vagina. Victim appears minimally responsive and stares at Martinez as Martinez proceeds to squeeze Victim's upper right thigh. Martinez continues his sexual assault of Victim, placing his right hand apparently up and inside Victim's shorts on, near, or penetrating Victim's vagina. Martinez then three times moves his hand in a continuous rubbing motion while it is inside Victim's shorts and on, near, or penetrating her vagina, before

pulling his hand back and squeezing her upper right thigh another time. Not finished sexually assaulting Victim, Martinez moves the seatbelt positioned across Victim's chest and squeezes her left breast (over her hoodie), before unzipping her hoodie, placing his right hand inside Victim's hoodie, and rubbing and squeezing Victim's left breast for several seconds. After groping Victim's breast, Martinez steps away from Victim and shuts the patrol vehicle door. Victim then appears to look up at the vehicle's backset camera several times.

16. Following my review of this video, I interviewed Victim who corroborated that on April 30, 2023, Martinez arrested her for driving while intoxicated and, after arresting and transporting her, sexually assaulted her while she was in his custody.<sup>2</sup> Victim also reported that following the sexual assault, Martinez, on at least two occasions, on May 2, 2023, and May 6, 2023, called her cellphone. Victim recorded these calls and saved the recordings. Victim provided me with the recordings, which I reviewed.

17. The following is a summary of the recorded call which Victim reported receiving on May 2, 2023: The caller, calling from a blocked number, identifies himself as "Michael." When Victim says, "Who is Michael?" the caller responds, "We met the other day." Victim again says that she does not know who is calling. The caller responds, "I went by your work, but you're not there." Victim asks how the caller knows where she works and he simply replies, "You work at the weed shop." Victim tells the caller that she is not good with names and is "concerned." The caller responds that he works for the "Sheriff's Department." Victim asks if the caller is calling just for fun, and he says that he is calling to see what she is doing and to tell

---

<sup>2</sup> This is a brief summary of the information I learned from Victim related to why probable cause exists to search Martinez's Apple iPhone accounts. I have not included all the information I learned from Victim during this interview.

her that the charges will be dismissed. Victim asks the caller if he is trying to hang out and he tells her to call him when she is alone. Victim says she can be alone later if he wants to hang out and they talk about timing. The caller then asks Victim step outside and asks her whether anyone can hear him. She tells him that no one can hear him, and he again tells her that the charges will be dismissed. The caller then asks Victim what she is thinking about, and she responds, "I'm thinking how you did that." The caller responds, "Oh, I'm just gonna dismiss that." Victim asks whether he can just do that, and he responds he can. Victim asks, "Oh, you're above the law?" The caller says he is not and changes the topic to asking Victim what she said she is wearing. The call ends with Martinez telling Victim, "Just don't tell anybody," and to just go to court, do what they say, and the charges will be dismissed in 30 days.

18. The following is a summary of the recorded call which Victim reported receiving on May 6, 2023: The caller, again calling from a blocked number, identifies himself as "Martinez." Victim asks the caller to repeat himself and the caller responds, "Martinez, who's this? Victim replies, "Who is this?" and the call ends.

19. Frightened that Martinez kept calling her from blocked numbers, Victim set her phone to not accept calls from private numbers. Victim has not spoken to or seen Martinez since May 6, 2023.

20. In addition to feeling unsafe due to the repeated calls from blocked numbers, Victim also felt harassed and unsafe due to the caller's statement that he went to her workplace. Victim reported that following the sexual assault and Martinez's calls, she stopped working at her place of employment, which she told me was Monster House on Solano Drive and stopped sleeping at her residence.



21. In addition to obtaining and reviewing the recovered footage of Martinez sexually assaulting Victim, during my investigation I also obtained and reviewed additional recovered footage from Martinez's patrol vehicle's WatchGuard DVR System. The recovered footage was dated April 30, 2023, and at the times listed on the footage, Martinez was off duty. In the footage, loud crashing sounds can be heard, and Martinez can be observed walking back and forth several times from his residence to his patrol vehicle. The last video, recorded at 9:51 p.m. that evening, shows a black screen and audio. This could indicate the WatchGuard DVR System was in the process of being damaged while the final video was being recorded. Based on my investigation, I believe this video shows Martinez attempting to damage the WatchGuard DVR System in his patrol vehicle, to conceal his sexual assault of Victim earlier that day.

22. In addition to reviewing this additional recovered footage, I interviewed a sergeant from the New Mexico State Police ("NMSP") (hereinafter "Witness 4"), who told me that in reviewing the recovered footage of Martinez sexually assaulting Victim, he observed Martinez wearing his DASO issued body worn DVR camera.<sup>3</sup> Witness 4 opined that Martinez may have purposely unplugged the camera lens attachment on his body worn camera during the sexual assault of Victim with the intent to prevent the body worn camera from properly functioning. I then spoke with another DASO officer (hereinafter "Witness 5") who explained that the DASO body worn DVR camera must be activated with a push of a button to function. He added that the body worn DVR camera has a lens attachment which, when connected and activated, allows for a recording to take place. Witness 5 reviewed the video of Martinez

---

<sup>3</sup> This is a different camera than the WatchGuard DVR system that was in Martinez's marked patrol vehicle.

sexually assaulting Victim and stated that he believed Martinez's body worn camera was on during the assault because he observed a green light on the camera. Witness 5, however, pointed out that the red flashing light feature on the camera indicated that while the device was turned on, it was not recording because the camera lens attachment was detached. Witness 5 opined that Martinez intentionally disconnected the lens attachment of his body worn camera so that the body worn camera would not function properly and thus would not record the sexual assault.

23. On September 19, 2023, United States Magistrate Judge Damian L. Martinez issued both a federal arrest warrant for Martinez and a federal search warrant for Martinez's cellular phone. (*See* Case Number 23-1817MR-search warrant; Case Number 23-1430MJ-arrest warrant).

24. Martinez was arrested by the FBI and other law enforcement without incident at the DASO headquarters. During Martinez's arrest, an Apple iPhone was located on his person and seized pursuant to the search warrant. In addition, during Martinez's arrest, I spoke with Martinez and asked him questions unrelated to the investigation. After hearing his voice, I confirmed that he was the caller of the phone calls placed to Victim from blocked numbers.

25. Pursuant to the terms of the issued federal search warrant for Martinez's cellular phone, after locating and seizing Martinez's Apple iPhone, I used the iPhone's facial recognition feature to open the iPhone so that the FBI could later perform a digital forensic extraction of the phone's contents.

26. Within days of seizure, the FBI CART (Computer Analysis Response Team) conducted a forensic extraction of Martinez's iPhone. FBI SA Sean Macmanus, who is assigned to the FBI's Cellular Analysis Survey Team (CAST), sent two preservation letters to Apple on September 22, 2023, for the ACCOUNTS.

27. On October 19, 2023, I reviewed portions of the forensic extraction of Martinez's Apple iPhone. During my review, I saw that on May 1, 2023, one day after Martinez detained and sexually assaulted Victim, the user of the Apple iPhone conducted a web search for "Monster House Dispensary." I recognized "Monster House" as the place where Victim told me she worked before the sexual assault. I also recalled hearing on the recorded call, which Victim reported receiving on May 2, 2023, the caller telling Victim that he went to her work but that she was not there and that he knew she worked at the weed shop. I conducted a web search of Monster House Dispensary and verified that Monster House Dispensary is located on Solano Drive in Las Cruces, New Mexico.

28. During my review, I also found that on May 2, 2023, at 3:19 p.m., Martinez's extraction timeline listed a phone number that I know is assigned to Victim's cellular phone. This finding corroborated Victim's statement to me that Martinez contacted Victim via a blocked phone number on May 2, 2023.

29. I then served a federal grand jury subpoena to Verizon for tolls records from the phone number associated with Martinez's Apple iPhone. After receiving and reviewing the results, I saw that the toll records corroborated Victim's account. Specifically, I observed that on May 2, 2023, the phone number associated with Martinez's Apple iPhone called Victim's phone twice, once at 3:42 p.m. and once at 3:44 p.m. On both calls, the user dialed \*67 to hide their phone number. On May 6, 2023, the phone number associated with Martinez's Apple iPhone again called Victim's phone at 10:07 p.m. Again, the user dialed \*67 to hide their phone number.

30. In addition, in reviewing the forensic extraction of Martinez's Apple iPhone, I also uncovered records revealing that the user of the iPhone conducted a web search on May 4,

2023, at 1:44 a.m. for <https://law.justia.com/codes/new-mexico/2018/chapter-30/article-9/section-30-9-12>. I conducted a web search of this website and found that it corresponds to the 2018 New Mexico Criminal Laws. Specifically, the site is for the New Mexico Sexual Offenses/Criminal Sexual Conduct. This search was conducted approximately four days after Martinez's sexual assault of the Victim and approximately two days after Martinez falsely reported that his DASO issued body worn camera was missing and that an unknown person had damaged his DASO patrol vehicle's WatchGuard DVR system.

31. Based on my training, experience, and investigation to date, I believe Martinez, while on duty for the DASO, sexually assaulted Victim while she was in his custody, handcuffed and restrained with a seatbelt inside the prisoner compartment of Martinez's patrol unit, thereby depriving the Victim of her civil rights. I also believe that after sexually assaulting Victim, Martinez attempted to destroy evidence of the sexual assault by falsely reporting that someone had stolen his DASO issued body worn camera and destroyed his DASO patrol vehicle WatchGuard DVR system, when Martinez knew that he himself had tampered with his WatchGuard DVR system.

32. I further believe that Martinez used his Apple iPhone in furtherance of the crimes he committed to find and stalk Victim. As the forensic extraction of Martinez's Apple iPhone and toll records reveal, Martinez used his Apple iPhone to call Victim multiple times, on different days, from a blocked number; to search for Victim's work location; and to obtain information about the New Mexico state laws governing sexual assaults, in an apparent attempt to edify himself on the potential criminal charges he could face for the crimes committed.

33. Based on my training and experience, I also believe that Apple maintains the described evidence and other records that may have not been recovered during the forensic

extraction of the Apple iPhone, which could be due to Martinez's efforts to delete them. This is particularly a concern as my investigation has already revealed that Martinez attempted to destroy other evidence of his sexual misconduct.

#### **BACKGROUND CONCERNING APPLE**<sup>4</sup>

34. Apple is a United States company that produces the iPhone, iPad, and iPod Touch, all of which use the iOS operating system, and desktop and laptop computers based on the Mac OS operating system.

35. Apple provides a variety of services that can be accessed from Apple devices or, in some cases, other devices via web browsers or mobile and desktop applications ("apps"). As described in further detail below, the services include email, instant messaging, and file storage:

a. Apple provides email service to its users through email addresses at the domain names mac.com, me.com, and icloud.com.

b. iMessage and FaceTime allow users of Apple devices to communicate in real-time. iMessage enables users of Apple devices to exchange instant messages ("iMessages") containing text, photos, videos, locations, and contacts, while FaceTime enables those users to conduct audio and video calls.

---

<sup>4</sup> The information in this section is based on information published by Apple on its website, including, but not limited to, the following document and webpages: "U.S. Law Enforcement Legal Process Guidelines," available at <https://www.apple.com/legal/privacy/law-enforcement-guidelines-us.pdf>; "Manage and use your Apple ID," available at <https://support.apple.com/en-us/HT203993>; "iCloud," available at <http://www.apple.com/icloud/>; "Introduction to iCloud," available at <https://support.apple.com/kb/PH26502>; "What does iCloud back up?," available at <https://support.apple.com/kb/PH12519>; and "Apple Platform Security," available at [https://help.apple.com/pdf/security/en\\_US/apple-platform-security-guide.pdf](https://help.apple.com/pdf/security/en_US/apple-platform-security-guide.pdf).

c. iCloud is a cloud storage and cloud computing service from Apple that allows its users to interact with Apple's servers to utilize iCloud-connected services to create, store, access, share, and synchronize data on Apple devices or via icloud.com on any Internet-connected device. For example, iCloud Mail enables a user to access Apple-provided email accounts on multiple Apple devices and on iCloud.com. iCloud Photo Library and My Photo Stream can be used to store and manage images and videos taken from Apple devices, and iCloud Photo Sharing allows the user to share those images and videos with other Apple subscribers. iCloud Drive can be used to store presentations, spreadsheets, and other documents. iCloud Tabs and bookmarks enable iCloud to be used to synchronize bookmarks and webpages opened in the Safari web browsers on all of the user's Apple devices. iCloud Backup allows users to create a backup of their device data. iWork Apps, a suite of productivity apps (Pages, Numbers, Keynote, and Notes), enables iCloud to be used to create, store, and share documents, spreadsheets, and presentations. iCloud Keychain enables a user to keep website username and passwords, credit card information, and Wi-Fi network information synchronized across multiple Apple devices.

d. Game Center, Apple's social gaming network, allows users of Apple devices to play and share games with each other.

e. Find My allows owners of Apple devices to remotely identify and track the location of, display a message on, and wipe the contents of iOS devices, as well as share their location with other iOS users. It also allows owners of Apple devices to manage, interact with, and locate AirTags, which are tracking devices sold by Apple.

f. Location Services allows apps and websites to use information from cellular, Wi-Fi, Global Positioning System (“GPS”) networks, and Bluetooth, to determine a user’s approximate location.

g. App Store and iTunes Store are used to purchase and download digital content. iOS apps can be purchased and downloaded through App Store on iOS devices, or through iTunes Store on desktop and laptop computers running either Microsoft Windows or Mac OS. Additional digital content, including music, movies, and television shows, can be purchased through iTunes Store on iOS devices and on desktop and laptop computers running either Microsoft Windows or Mac OS.

36. Apple services are accessed through the use of an “Apple ID,” an account created during the setup of an Apple device or through the iTunes or iCloud services. The account identifier for an Apple ID is an email address, provided by the user. Users can submit an Apple-provided email address (often ending in @icloud.com, @me.com, or @mac.com) or an email address associated with a third-party email provider (such as Gmail, Yahoo, or Hotmail). The Apple ID can be used to access most Apple services (including iCloud, iMessage, and FaceTime) only after the user accesses and responds to a “verification email” sent by Apple to that “primary” email address. Additional email addresses (“alternate,” “rescue,” and “notification” email addresses) can also be associated with an Apple ID by the user. A single Apple ID can be linked to multiple Apple services and devices, serving as a central authentication and syncing mechanism.

37. Apple captures information associated with the creation and use of an Apple ID. During the creation of an Apple ID, the user must provide basic personal information including the user’s full name, physical address, and telephone numbers. The user may also provide means

of payment for products offered by Apple. The subscriber information and password associated with an Apple ID can be changed by the user through the “My Apple ID” and “iForgot” pages on Apple’s website. In addition, Apple captures the date on which the account was created, the length of service, records of log-in times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to and utilize the account, the Internet Protocol address (“IP address”) used to register and access the account, and other log files that reflect usage of the account.

38. Additional information is captured by Apple in connection with the use of an Apple ID to access certain services. For example, Apple maintains connection logs with IP addresses that reflect a user’s sign-on activity for Apple services such as iTunes Store and App Store, iCloud, Game Center, and the My Apple ID and iForgot pages on Apple’s website. Apple also maintains records reflecting a user’s app purchases from App Store and iTunes Store, “call invitation logs” for FaceTime calls, “capability query logs” for iMessage, and “mail logs” for activity over an Apple-provided email account. Records relating to the use of the “Find My” service, including connection logs and requests to remotely find, lock, or erase a device, are also maintained by Apple.

39. Apple also maintains information about the devices associated with an Apple ID. When a user activates or upgrades an iOS device, Apple captures and retains the user’s IP address and identifiers such as the Integrated Circuit Card ID number (“ICCID”), which is the serial number of the device’s SIM card. Similarly, the telephone number of a user’s iPhone is linked to an Apple ID when the user signs into FaceTime or iMessage. Apple also may maintain records of other device identifiers, including the Media Access Control address (“MAC address”), the unique device identifier (“UDID”), and the serial number. In addition,



information about a user's computer is captured when iTunes is used on that computer to play content associated with an Apple ID, and information about a user's web browser may be captured when used to access services through icloud.com and apple.com. Apple also retains records related to communications between users and Apple customer service, including communications regarding a particular Apple device or service, and the repair history for a device.

40. Apple provides users with five gigabytes of free electronic space on iCloud, and users can purchase additional storage space. That storage space, located on servers controlled by Apple, may contain data associated with the use of iCloud-connected services, including: email (iCloud Mail); images and videos (iCloud Photo Library, My Photo Stream, and iCloud Photo Sharing); documents, spreadsheets, presentations, and other files (iWork and iCloud Drive); and web browser settings and Wi-Fi network information (iCloud Tabs and iCloud Keychain). iCloud can also be used to store iOS device backups, which can contain a user's photos and videos, iMessages, Short Message Service ("SMS") and Multimedia Messaging Service ("MMS") messages, voicemail messages, call history, contacts, calendar events, reminders, notes, app data and settings, Apple Watch backups, and other data. Some of this data is stored on Apple's servers in an encrypted form but may nonetheless be decrypted by Apple. Records and data associated with third-party apps, including the instant messaging service WhatsApp, may also be stored on iCloud.

41. In federal investigations of civil rights and color of law violations, I know that subjects often attempt to cover up their crimes by destroying evidence and convincing witnesses to not report incidents to law enforcement. Among other evidence, I believe that Apple may possess evidence indicative of Martinez's location when he attempted to find Victim at her place

of employment to tell her that the charges against her would be dismissed. I believe that Martinez did this to ease the Victim's concerns about her pending criminal charges in exchange for an agreement to not reveal his sexual assault of her. I also believe that Apple may possess evidence of additional sexual misconduct committed by Martinez. In my training and experience, evidence of who was using an Apple ID and from where, and evidence related to criminal activity of the kind described above, may be found in the files and records described above. This evidence may establish the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or, alternatively, to exclude the innocent from further suspicion.

42. Based on my review of toll records, the recorded phone calls to Victim, and my review of the forensic extraction of Martinez's Apple iPhone, Martinez, on more than one day and in more than one way, used his Apple iPhone to find and speak with Victim after sexually assaulting her. Data and records further evidencing Martinez's attempts to find and talk to Victim in the days after the sexual assault may be maintained by Apple in the iCloud, as most Apple iPhone users save various types of information in their iCloud accounts. There may also be additional information about other attempts by Martinez, in the days, weeks, and months after the sexual assault, to contact Victim that both the Victim (due to, among things, blocking her phone from accepting calls from private numbers) and law enforcement are unaware of. For example, the stored communications and files connected to Martinez's Apple ID/iCloud accounts may provide direct evidence of the offenses under investigation. Based on my training and experience, instant messages, emails, voicemails, photos, videos, and documents are often created and used in furtherance of criminal activity, including to communicate and facilitate the offenses under investigation.

43. In addition, the user's account activity, logs, stored electronic communications, and other data retained by Apple can indicate who has used or controlled the account. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, subscriber information, email and messaging logs, documents, and photos and videos (and the data associated with the foregoing, such as geo-location, date, and time) may be evidence of who used or controlled the account at a relevant time. As an example, because every device has unique hardware and software identifiers, and because every device that connects to the Internet must use an IP address, IP address and device identifier information can help to identify which computers or other devices were used to access the account. Such information also allows investigators to understand the geographic and chronological context of access, use, and events relating to the crime under investigation.

44. Account activity may also provide relevant insight into the account owner's state of mind as it relates to the offenses under investigation. For example, information on the account may indicate the owner's motive and intent to commit a crime (e.g., information indicating a plan to commit a crime), or consciousness of guilt (e.g., deleting account information in an effort to conceal evidence from law enforcement).

45. Other information connected to an Apple ID may lead to the discovery of additional evidence. For example, the identification of apps downloaded from App Store and iTunes Store may reveal services used in furtherance of the crimes under investigation. In addition, emails, instant messages, Internet activity, documents, and contact and calendar information can lead to the identification of co-conspirators and instrumentalities of the crimes under investigation.

46. As described above, my investigation concerns the sexual assault, committed under color of law, of a female victim who was in the perpetrator's custody at the time of the assault and the perpetrator's attempted destruction of evidence and witness tampering after the commission of the crime. During a search of the forensic extraction of Martinez's Apple iPhone, I found evidence that Martinez had used his iPhone to call the victim of the sexual assault multiple times, on different days, from a blocked number; to search for the victim's work location; and to obtain information about the New Mexico state laws governing sexual assaults, in an apparent attempt to edify himself on the potential criminal charges he could face for the crimes committed. Therefore, Apple's servers are likely to contain stored electronic communications and information concerning subscribers and their use of Apple's services. In my training and experience, such information may constitute evidence of the crimes under investigation including information that can be used to identify the account's user.


[See next page...]

**CONCLUSION**

47. Based on the foregoing, I request that the Court issue the proposed search warrant.

48. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant. The government will execute this warrant by serving the warrant on Apple. Because the warrant will be served on Apple, who will then compile the requested records at a time convenient to it, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night.

Respectfully submitted,



\_\_\_\_\_  
Armida Maria Macmanus  
Special Agent  
Federal Bureau of Investigation

Sworn telephonically, signed remotely, and transmitted by email on  
October 25, 2023, 2023



\_\_\_\_\_  
Honorable Jerry H. Ritter  
UNITED STATES MAGISTRATE JUDGE